UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,928	02/17/2004	John L. Moss	S2-002AUS	9369

36543 7590 06/23/2008

S2 SECURITY CORPORATION
50 Speen St.
Suite 300
Framingham, MA 01701

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,928	MOSS ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 16 March 2008.

2. Claims 1-20 are pending in the application.

3. Claims 1-20 have been rejected.

Response to Amendment

4. The examiner approves of the amendment made to claim 5. There is no longer any misspelling issue. The examiner withdraws the objection to claim 5.

Response to Arguments

5. Applicant's arguments filed 16 March 2008 have been fully considered but they are not persuasive.

On page 5, the applicant argues that Brooks does not teach "a network security controller". The applicant argues that Brooks does not teach "a relational database including portal objects".

The examiner respectfully disagrees. Brooks discloses the security evaluation or audit can by conducted by one or more independent evaluators or auditors. A map or schematic of the airport facility can be used to assign identification numbers or other identifiers to the various areas, spaces and access points. This information can be input into a computer system that can be used to collect the data. The computer system can include one or more portable computers, cell phone or a personal digital assistants (PDA) or other portable device. The information can be stored in a data structure (e.g. a database, table, XML document, etc.) on each computer and downloaded to a data structure at a central repository computer for analysis and further processing. Alternatively, each computer can connected to a wired or wireless network and

adapted for transferring the data to a repository computer within the computer system in real time or on a periodic basis. During the course of the evaluation or audit, the portable computer or PDA can be programmed to prompt the evaluator or auditor for information relating to the various attributes of each component (area or access point) of the facility. The program can also limit and/or check the integrity of the input of information to that which is permitted for each attribute evaluated, in order to improve the integrity of the data collected. The repository computer can further be programmed to analyze and review the data as it is received in order identify possible data errors that can be corrected while the evaluators or auditors are still on site.

On page 6, the applicant argues that Brooks does not disclose a network node. The applicant argues that Brooks does not teach “a local database”, "an event generator coupled to the local database" or "a finite state portal”.

The examiner respectfully disagrees. Brooks discloses a wireless network. The examiner asserts that it is well known in the art that wireless networks contain network nodes. As discussed above, Brooks discloses a repository computer for gathering data. Brooks discloses the event generator and a finite state portal. Brooks discloses a system can also monitor the access of person throughout the facility to detect events that might warrant further investigation. For example, where a person's badge entering a first location and then entering a second location within a short period of time when the distance between the locations is large enough to suggest that a badge has been copied or that an intermediate access point did not record the person passing through. In addition, the system may record that a person accessed a particular location on a particular day when they were not scheduled to work that day, would trigger an event that might warrant further investigation.

On page 7, the applicant argues that Brooks does not teach a protocol normalizer. The applicant argues that Brooks does not teach "node local database downloads an extensible markup language representation of the predetermined resource information".

The examiner respectfully disagrees. Brooks discloses that after all the information is gathered and the security values for each component are determined, an overall score for the facility can be calculated at step 116. The overall score can be determined as a function of the security values, the security ratings and the attributes. In one embodiment, several ratings can be determined, a simple rating which consists of the sum of the products of the security values and the security rating for each component of the facility. A more comprehensive rating can attempt to weight the different components and the security values and ratings associated with them. In addition, the security rating could be normalized or averaged in order to compare it to other similar or dissimilar facilities. Brooks discloses the security evaluation or audit can by conducted by one or more independent evaluators or auditors. A map or schematic of the airport facility can be used to assign identification numbers or other identifiers to the various areas, spaces and access points. This information can be input into a computer system that can be used to collect the data. The computer system can include one or more portable computers, cell phone or personal digital assistants (PDA) or other portable device. The information can be stored in a data structure (e.g. a database, table, XML document, etc.) on each computer and downloaded to a data structure at a central repository computer for analysis and further processing.

On page 8, the applicant argues that Brooks is silent as to processing at least one portal even in a finite state portal controller. The applicant argues that Brook does not suggest or teach any of the steps occurring on a network node including steps involving local actions. The

applicant argues that Brooks is silent as to "storing predetermined resource information from at least one resource table of a relational database in a local data base" and "mapping the field device signal to the at least one portal event using the stored predetermined resource information". The applicant argues that Brooks does not disclose "detecting a state change in the field device signal to provide a portal even; and translating the field device signal to provide a portal event".

The examiner respectfully disagrees. As defined by the applicant, a portal event is an event occurring at a physical opening or area under access control and/or supervision. As discussed above, Brooks discloses a person's badge entering a first location and then entering a second location within a short period of time when the distance between the locations is large enough to suggest that a badge has been copied or that an intermediate access point did not record the person passing through. In addition, the system may record that a person accessed a particular location on a particular day when they were not scheduled to work that day, would trigger an event that might warrant further investigation. Brooks discloses an example where the visa of an individual has expired, for example, the system can alert the appropriate authorities and allow them to take appropriate action. The information can also be used to reduce the ability of people to use false identification at these and other locations where the person's biometric data can be used to verify their identity. Brooks discloses the attribute data, including biometric and other data can be forwarded to the global profile data store 320 which allows for distribution to many facilities. This system can also allow for detection of false or duplicate identification by having each facility report the detection of each individual to the global profile data store 320 where a system 324 can analyze the information to identify the travel of predetermined persons,

such as those with expired visas or travel papers. Similarly, where the system detects that the same person is identified as passing through two distant locations at essentially the same time or within an unreasonably small amount of time, it can presumed that one is using a false identification. Additional analysis of this information can be conducted to determine suspect travel patterns and anticipate suspect activity. Preferably, this is conducted by a government or independent agency which can protect the privacy of the people who's information is stored in the system. Brooks discloses analyzing the evaluation data, identifying the components that receive the lowest ratings and for identifying modifications to the existing security measures to improve the evaluation of the component and the facility and for prioritizing the same. In accordance with the invention, the method and system includes analyzing the data gathered during the evaluation process and identifying the components that have the lowest security values and using the data gathered, identify the modifications that are compatible and likely to improve the security value of the component. Thus, for example, where an access door is locked with a mechanical lock and key mechanism, the security value can be improved by providing a surveillance camera to monitor the door or by providing a numeric keypad in addition to the mechanical lock or any other method or apparatus, thus providing an additional level of security.

On page 9, the applicant argues that Brooks does not teach receiving a command; mapping the command using the predetermined resource information to provide a command portal event; processing the command portal event in the finite state portal controller to provide at least one local action; and converting the local action into a local action field device signal directed to a selected application extension.

The examiner respectfully disagrees. As discussed above, Brooks discloses analyzing the evaluation data, identifying the components that receive the lowest ratings and for identifying modifications to the existing security measures to improve the evaluation of the component and the facility and for prioritizing the same. In accordance with the invention, the method and system includes analyzing the data gathered during the evaluation process and identifying the components that have the lowest security values and using the data gathered, identify the modifications that are compatible and likely to improve the security value of the component. Thus, for example, where an access door is locked with a mechanical lock and key mechanism, the security value can be improved by providing a surveillance camera to monitor the door or by providing a numeric keypad in addition to the mechanical lock or any other method or apparatus, thus providing an additional level of security.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-10 and 12-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Brooks et al US 2003/0210139 A1.

As to claim 1, Brooks et al discloses an integrated security system operating over a network comprising:

a network security controller [0038] coupled to the network comprising:

a relational database including portal objects and related resources represented in at least one table in the relational database [0031];

at least one network node comprising:

a local database coupled to the network adapted to receive predetermined resource information from the relational database [0031];

an event generator coupled to the local database to provide at least one portal event in response to the predetermined resource information received by the local database [0037]; and

a finite state portal controller coupled to the network and the event generator for providing at least one of an action and a global event in response to the at least one portal event [0046].

As to claim 2, Brooks et al discloses that the event generator comprises a protocol normalizer [0032].

As to claim 3, Brooks et al discloses that the event generator further comprises a data stream converter coupled to the protocol normalizer adapted to receive data from a field device [0032].

As to claim 4, Brooks et al discloses that the field device is a reader module [0038].

As to claim 5, Brooks et al discloses that the event generator comprises:

a supervision controller [0042];

an I/O controller coupled to the supervision controller and adapted to receive signals from an input extension [0042].

As to claim 6, Brooks et al discloses a network node controller coupled to the database and coupled to the at least one network node [0031].

As to claim 7, Brooks et al discloses that the network security controller further comprises an extensible markup language generator and the at least one network node local database downloads an extensible markup language representation of the predetermined resource information [0035].

As to claim 8, Brooks et al discloses that the extensible markup language representation comprises XML [0035].

As to claim 9, Brooks et al discloses that the at least one global event is represented using an extensible markup language representation [0035].

As to claim 10, Brooks et al discloses that the extensible markup language representation comprises XML [0035].

As to claim 12, Brooks et al discloses a method to normalize an access control event comprising:

converting a field device signal representing the access control event to a data stream [0032];

normalizing the data stream to provide at least one portal event [0032]; and

processing the at least one portal event in a finite state portal controller to provide at least one of a local action and a global event [0037].

As to claim 13, Brooks et al discloses the method further comprising:

storing predetermined resource information from at least one resource table of a relational database in a local database [0031]; and

wherein normalizing the data stream comprises mapping the field device signal to the at least one portal event using the stored predetermined resource information [0032].

As to claim 14, Brooks et al discloses using an extensible markup language representation for the predetermined resource information [0035].

As to claim 15, Brooks et al discloses that mapping the field device signal comprises at least one of:

detecting a state change in the field device signal to provide a portal event [0044]; and

translating the field device signal to provide a portal event [0044].

As to claim 16, Brooks et al discloses processing the at least one local action in response to determining that the field is a module [0039].

As to claim 17, Brooks et al discloses a method to process an access control event from an application extension comprising:

supervising the application extension to provide at least one portal event [0032]; and

processing the at least one portal event in a finite state portal controller to provide at least one of a local action and a global event [0037].

As to claim 18, Brooks et al discloses the method further comprising:

storing predetermined resource information from at least one resource table of a relational database in a local database [0035]; and

mapping an application extension state change signal to provide the at least one portal event [0035].

As to claim 19, Brooks et al discloses using an extensible markup language representation for the predetermined resource information [0035].

As to claim 20, Brooks et al discloses the method further comprising:

receiving a command [0039-0046];

mapping the command using the predetermined resource information to provide a command portal event [0039-0046];

processing the command portal event in the finite state portal controller to provide at least one local action [0039-0046]; and

converting the local action into a local action field device signal directed to a selected application extension [0039-0046].

1 17.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brooks et al US 2003/0210139 A1 as applied to claim 1 above, and further in view of Elwahab et al US 2001/0034754 A1.

As to claim 11, Brooks et al does not teach that the network security controller further comprises a web server coupled to the network and the database to provide at least one user interface to the integrated security system in at least one browser.

Elwahab et al teaches a web server coupled to the network and the database to provide at least one user interface to the integrated security system in at least one browser [0025-0026].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brooks et al so that the network security controller would have comprised a web server coupled to the network and the database to provide at least one user interface to the integrated security system in at least one browser.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brooks et al by the teaching of Elwahab et al because it allows a user to gain access and control devices without a computer having a specific application software loaded thereon [0007].

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131